

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 06-216897

(43)Date of publication of application : 05.08.1994

(51)Int.Cl.

H04L 9/06

H04L 9/14

G09C 1/00

(21)Application number : 05-024750

(71)Applicant : NIPPON SIGNAL CO LTD:THE

(22)Date of filing : 20.01.1993

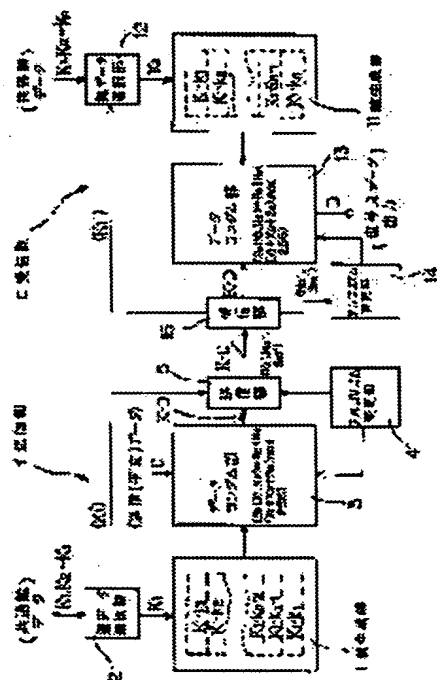
(72)Inventor : AOYANAGI HIDEYUKI

(54) DATA TRANSMITTER-RECEIVER

(57)Abstract:

PURPOSE: To allow the transmitter-receiver to cope with a fact that the strength of ciphering is high and a common key might be decoded by storing plural common key data in advance and revising the common key under a prescribed condition.

CONSTITUTION: A sender side is provided with a key generating section 1 generating plural kinds of sub keys based on a prescribed common key K1. The common key K1 fed to the key generating section 1 is selected alternatively by a key data selection section 2 from plural common keys K1-Kn stored in advance in a memory of a transmission side and a data random section 3 uses sub keys K1.K1-K1.Kn of the key generating section 1 to generate a ciphered sentence K/D according to a prescribed algorithm from transmission data D. A key data generating section 11 on a receiver side generates plural kinds of sub keys K1.K1-K1.Kn based on the common key K1 and a data random section 13 decodes the ciphered sentence K.D received from a reception section 15 according to a prescribed algorithm. The key data selection section 2 on the sender side selects a common key under a certain condition such as that after lapse of prescribed time.



LEGAL STATUS

[Date of request for examination] 24.12.1999

[Date of sending the examiner's decision of rejection] 28.01.2003

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's

BEST AVAILABLE COPY

This Page Blank (uspto)

decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

This Page Blank (uspto)

(51)Int.Cl. ⁵	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 L 9/06				
	9/14			
G 0 9 C 1/00		8837-5L		
		7117-5K		
			H 0 4 L 9/ 02	Z
審査請求 未請求 請求項の数 3 F D (全 5 頁)				

(21)出願番号 特願平5-24750

(22)出願日 平成5年(1993)1月20日

(71)出願人 000004651

日本信号株式会社

東京都千代田区丸の内3丁目3番1号

(72)発明者 青柳 秀幸

埼玉県浦和市上木崎1丁目13番8号 日本

信号株式会社与野事業所内

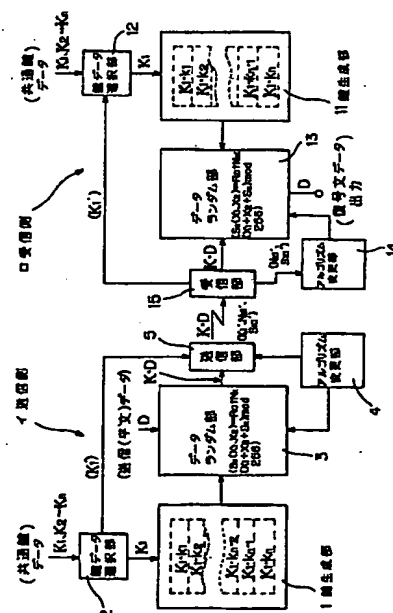
(74)代理人 弁理士 石井 光正

(54)【発明の名称】 データ送受信装置

(57)【要約】

【目的】 共通鍵が解読されたとしても、すぐに別の共通鍵に変更できるとともに、データランダム部のアルゴリズムも変更可能にして、極めて暗号強度の高いデータ送受信装置を得る。

【構成】 送信側から送信する所定の送信データを所定の共通鍵データを基にデータランダム部に格納されている所定のアルゴリズムに従って暗号化したのち受信側に送出し、又はその受信側で受信したその暗号文データをその所定の共通鍵データを基にデータランダム部に格納されている所定のアルゴリズムに従って復号処理して平文データを抽出するデータ送受信装置であって、複数の共通鍵データを予め格納する鍵データ格納手段と、所定時間経過等の所定の条件下で、前記鍵データ格納手段から所定の共通鍵データを選択する鍵データ選択手段と、前記データランダム部に格納されている所定のアルゴリズムを所定時間経過等の所定の条件下で変化させるアルゴリズム変更手段とを有している。



【特許請求の範囲】

【請求項1】 送信側から送信する所定の送信データを所定の共通鍵データを基にデータランダム部に格納されている所定のアルゴリズムに従って暗号化したのち受信側に送出し、又はその受信側で受信したその暗号文データをその所定の共通鍵データを基にデータランダム部に格納されている所定のアルゴリズムに従って復号処理して平文データを抽出するデータ送受信装置において、複数の共通鍵データを予め格納する鍵データ格納手段と、

所定時間経過等の所定の条件下で、前記鍵データ格納手段から所定の共通鍵データを選択する鍵データ選択手段と、

を設けたことを特徴とするデータ送受信装置。

【請求項2】 送信側から送信する所定の送信データを所定の共通鍵データを基にデータランダム部に格納されている所定のアルゴリズムに従って暗号化したのち受信側に送出し、又はその受信側で受信したその暗号文データをその所定の共通鍵データを基にデータランダム部に格納されている所定のアルゴリズムに従って復号処理して平文データを抽出するデータ送受信装置において、前記データランダム部に格納されている所定のアルゴリズムを所定時間経過等の所定の条件下で変化させるアルゴリズム変更手段を設けたことを特徴とするデータ送受信装置。

【請求項3】 送信側から送信する所定の送信データを所定の共通鍵データを基にデータランダム部に格納されている所定のアルゴリズムに従って暗号化したのち受信側に送出し、又はその受信側で受信したその暗号文データをその所定の共通鍵データを基にデータランダム部に格納されている所定のアルゴリズムに従って復号処理して平文データを抽出するデータ送受信装置において、複数の共通鍵データを予め格納する鍵データ格納手段と、

所定時間経過等の所定の条件下で、前記鍵データ格納手段から所定の共通鍵データを選択する鍵データ選択手段と、

前記データランダム部に格納されている所定のアルゴリズムを所定時間経過等の所定の条件下で変化させるアルゴリズム変更手段と、

を設けたことを特徴とするデータ送受信装置。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は、データ送受信装置に係り、特に暗号強度が高く、例えば、通信機能を備えたICカード型の非接触式定期券を用いる自動改札システムに好適なものに関する。

【0002】

【従来の技術】 従来、交信するデータの秘密を保持するために、データ内容を暗号化して通信を行うことが行

れている。この場合、通常、共通鍵暗号通信方式が採用されている。

【0003】 共通鍵暗号通信方式は、受信相手Aに送信すべきデータ（以下、平文データというときもある）Dがあるとき、先ず、受信相手Aと共通の共通鍵データ（以下、共通鍵という） K_C を用いて暗号文 $K_C \cdot D$ を作り、この暗号文 $K_C \cdot D$ を受信相手Aに送信し、他方、暗号文 $K_C \cdot D$ を受信した受信相手Aは、暗号文 $K_C \cdot D$ を共通鍵 K_C を用いて復号処理してデータDを抽出するようにしている。

【0004】 この共通鍵方式のデータ送受信装置においては、通常、鍵生成部において共通鍵 K_C を基にサブ鍵を多種生成するとともに、その生成されたサブ鍵を用いてデータランダム部で所定のアルゴリズムに従って平文データDを暗号化したり、又は復号化するようにしている。

【0005】 ところで、非接触式定期券は、磁気カード式の定期券に比べ、記憶容量が大きいので、定期券の機能の他に、例えば駅の売店等で買物もできるようなストアード・フェアカードとしての機能も持たせることが考えられる。このような多機能型とすると、非接触式定期券はもはや単なる定期券ではなくなり、一種の金券の性格を有するので、データの改ざんを困難にして安全性を確保することが望まれている。このため、自動改札機と非接触式定期券との間で交信されるデータを暗号化することが考えられている。

【0006】

【発明が解決しようとする課題】 しかしながら、共通鍵データを用いて暗号文化してデータ授受を行うデータ送受信装置においては、一旦、共通鍵が解読されてしまうと、データの改ざんを許してしまうこととなる。

【0007】 このような不正を阻止する手段としては、共通鍵のビット数を多くして、解読を困難にし、暗号強度を高めることも考えられる。

【0008】 しかし、単にビット数を多くしても、共通鍵が解読されたときは、データ送受信装置のシステムを変更しなければならない。

【0009】 殊に、非接触式自動改札システムにおいて、共通鍵が解読されたときは、システム変更の対象となる機器類が膨大であるため、大変な費用を必要とする。

【0010】 そこで、本発明は、上記問題点を解決するためになされたものであって、その目的は、暗号強度が高く、仮りに共通鍵が解読されたとしても、速やかに対応できるデータ送受信装置を提供することにある。

【0011】

【課題を解決するための手段】 本発明に係るデータ送受信装置は、送信側から送信する所定の送信データを所定の共通鍵データを基にデータランダム部に格納されている所定のアルゴリズムに従って暗号化したのち受信側に

送出し、又はその受信側で受信したその暗号文データをその所定の共通鍵データを基にデータランダム部に格納されている所定のアルゴリズムに従って復号処理して平文データを抽出するデータ送受信装置において、複数の共通鍵データを予め格納する鍵データ格納手段と、所定時間経過等の所定の条件下で、前記鍵データ格納手段から所定の共通鍵データを選択する鍵データ選択手段とを設けたことを特徴としている。また、前記データランダム部に格納されている所定のアルゴリズムを所定時間経過等の所定の条件下で変化させるアルゴリズム変更手段を設けたことを特徴としている。さらに、複数の共通鍵データを予め格納する鍵データ格納手段と、所定時間経過等の所定の条件下で、前記鍵データ格納手段から所定の共通鍵データを選択する鍵データ選択手段と、前記データランダム部に格納されている所定のアルゴリズムを所定時間経過等の所定の条件下で変化させるアルゴリズム変更手段とを設けたことを特徴としている。

【0012】

【作用】上記構成において、鍵データ選択手段は、所定の条件下で共通鍵データを変更する。したがって、それまでの共通鍵は無効となり、それまで使用されていた共通鍵が解読されても支障が生じない。また、アルゴリズム変更手段は、所定の条件下で平文データを暗号化するアルゴリズムを変更する。したがって、仮に共通鍵が解読され、かつ暗号文が復号化できたとしても、アルゴリズム変更後は、暗号文の復号化が困難となる。さらに鍵データ選択手段とアルゴリズム変更手段とを備えると、暗号強度は格段に向上する。

【0013】

【実施例】以下、本発明の実施例を図面に基いて説明する。図1は、一実施例装置の概略構成を示すブロック図であって、送信側イには、所定の共通鍵（図示の例では K_1 ）を基に複数種のサブ鍵 $K_1 \cdot k_1 \sim K_1 \cdot k_n$ を生成する鍵生成部1が設けられている。

【0014】鍵生成部1に供給される共通鍵 K_1 は、送信側イに設けられている図示しないメモリに予め格納されている複数の共通鍵 $K_1 \sim K_n$ から、鍵データ選択部2により択一的に選択されるように構成されている。

【0015】データランダム部3は、鍵生成部1のサブ鍵 $K_1 \cdot k_1 \sim K_1 \cdot k_n$ を用いて、平文データDを所定のアルゴリズムに従って暗号文 $K \cdot D$ を生成するように構成されている。

【0016】このアルゴリズムは、共通鍵暗号方式として一般的に用いられているフェイル（Feal）-8方式のf関数のS-ボックス（BOX）が格納されている。周知のS-BOXは、 $S_1(X_1, X_2) = \text{Rot}_2(X_1 \times X_2 + S_1) \bmod 256$ であるが、本実施例のS-BOXは、式中の「2」及び「 S_1 」がアルゴリズム変更部4によって変更されるように、つまり、 $S \times (X_1, X_2) = \text{Rot}_{N_x}(X_1 + X_2 + S_x) \bmod 256$ に構成されている。

od 256に構成されている。

【0017】送信部5は、周知の増幅器を備えて構成され、データランダム部3からの暗号文 $K \cdot D$ を受信側Dへ送信できるように構成されているとともに、受信側イで使用中の共通鍵（図示の例では K_1 ）の選択データ（ K_1' ）と、使用中のアルゴリズムの変数識別データ（ N_x' , S_x' ）を受信側ロへ送出するように構成されている。

【0018】受信側ロには、送信側イと同一構成の鍵生成部11、鍵データ選択部12、データランダム部13及びアルゴリズム変更部14を備えているとともに、送信側イの送信部5に対応した受信部15を備えている。また、送信側イの図示しないメモリには、送信側イと同様に複数の共通鍵 $K_1, K_2 \dots K_n$ が予め格納されている。

【0019】次に、本実施例装置の動作について説明する。今、鍵データ選択部2は、共通鍵 K_1 を選択し、かつアルゴリズム変更部4はS-BOXの変数を N_{x1} , S_{x1} を選択しているものとする。したがって、送信部5からは使用中の共通鍵とアルゴリズムを識別するための信号（ K_1' , N_{x1}' , S_{x1}' ）が受信側ロに送出される。

【0020】鍵生成部1では、選択された共通鍵 K_1 を用いて複数種（Feal-8の場合は8個）のサブ鍵 $K_1 \cdot k_1 \sim K_1 \cdot k_n$ を生成し、データランダム部3では、これらサブ鍵 $K_1 \cdot k_1 \sim K_1 \cdot k_n$ を用いて変数 N_{x1} , S_{x1} のアルゴリズムに従って平文データDを暗号文 $K \cdot D$ に変換する。そして、この暗号文 $K \cdot D$ は、送信部5から受信側ロへ送出される。

【0021】受信部5は、受信信号から使用中の共通鍵データ（ K_1' ）と使用中アルゴリズムの識別データ（ N_{x1}' , S_{x1}' ）を鍵データ選択部12及びアルゴリズム変更部14にそれぞれ送出する。したがって、鍵データ選択部12は、共通鍵 K_1 を選択するとともに、データランダム部13は変数 N_{x1} , S_{x1} を選択する。

【0022】鍵データ生成部11は、共通鍵 K_1 に基づいて複数種のサブ鍵 $K_1 \cdot k_1 \sim K_1 \cdot k_n$ を生成するとともに、データランダム部13は、受信部15から入力した暗号文 $K \cdot D$ を変数 N_{x1} , S_{x1} の所定のアルゴリズムに従って復号処理して復号文Dを抽出する。

【0023】送信側イの鍵データ選択部2及びアルゴリズム変更部4は、一定の条件下で、例えば所定時間経過後に、あるいは、当日の天候の状態による等の全く不規則的に共通鍵を選択し、さらにアルゴリズムを変更するようにしてある。

【0024】したがって、第三者が故意に一時的に使用されている共通鍵及びアルゴリズムを膨大な時間と費用を費やして解読したときには、既に、別の共通鍵とアルゴリズムが使用されているので、その解読は全く意味をなさないこととなる。このため、極めて暗号強度の高い

データ送受信装置とすることができる。

【0025】なお、上述の実施例では、共通鍵とアルゴリズムを同時に変更するようにしたが、どちらか一方だけでもよく、又は両者を交互に変更するようにしてもよい。

【0026】

【発明の効果】本発明に係るデータ送受信装置は、共通鍵又はデータランダム部のアルゴリズムを所定の条件下で変更するようにしたので、極めて暗号強度が高く、仮に共通鍵が解読されても、すぐに他の共通鍵に変更することが可能である。また、共通鍵とアルゴリズムの両方を変更するようにすると、より暗号強度を高めることが可能となる。

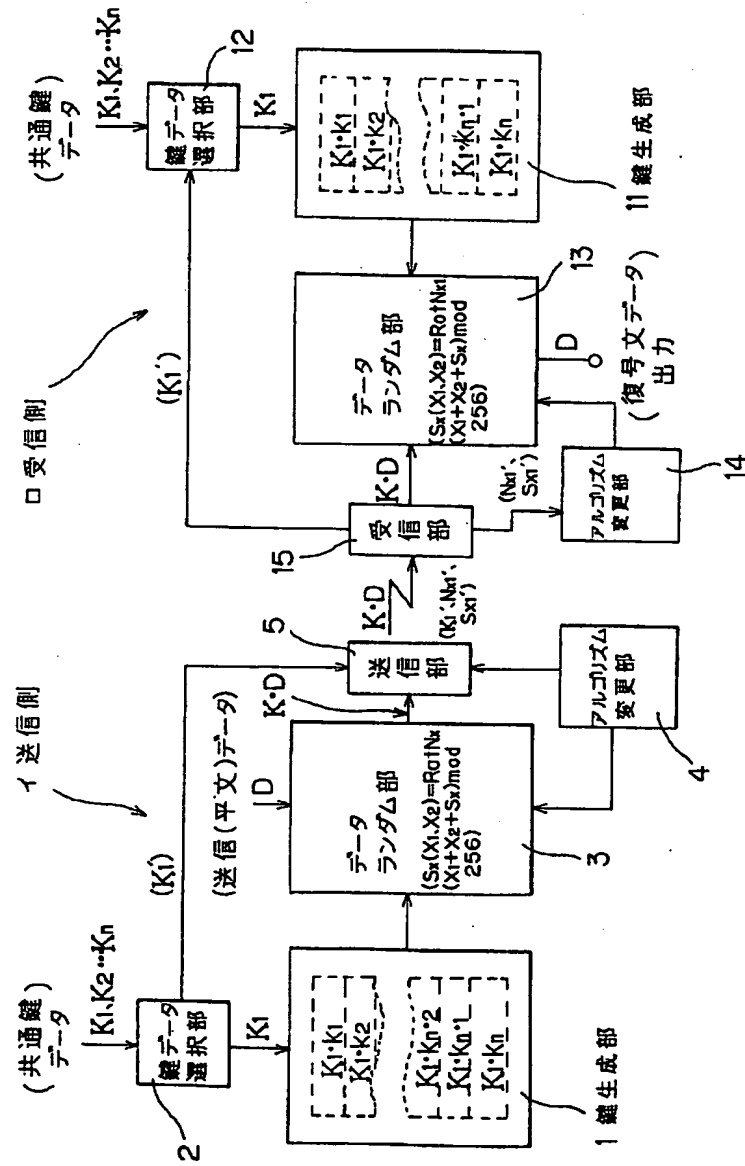
【図面の簡単な説明】

【図1】本発明の一実施例装置の概略構成を示すブロック図である。

【符号の説明】

1, 1 1	鍵生成部
2, 1 2	鍵データ選択部（鍵データ選択手段）
3, 1 3	データランダム部
4, 1 4	アルゴリズム変更部（アルゴリズム変更手段）
10 5	送信部
1 5	受信部
イ	送信側
ロ	受信側

【図1】



This Page Blank (uspto)

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☒ FADED TEXT OR DRAWING
- ☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

This Page Blank (uspto)